

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-117744

(43)Date of publication of application : 27.04.2001

(51)Int.Cl.

G06F 3/12

B41J 29/38

G06F 13/00

(21)Application number : 11-294452

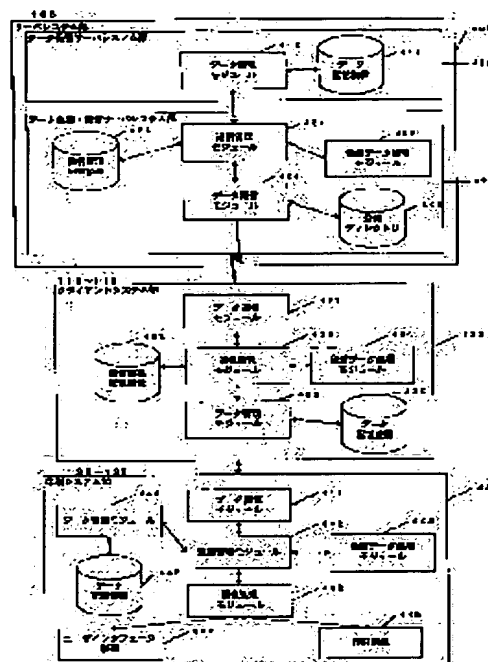
(71)Applicant : CANON INC

(22)Date of filing : 15.10.1999

(72)Inventor : SATO MASAYUKI  
SHIMONO MASAKI  
OSHIMA HAJIME  
TAKAKU MASAHIKO

## (54) PRINTING SYSTEM, PRINTING METHOD AND RECORDING MEDIUM

## (57)Abstract:

**PROBLEM TO BE SOLVED:** To provide a printing system capable of protecting inputted data up to the printing of the data.**SOLUTION:** The printing system has an input means for inputting protected data and information expressing the protection format of the protected data, a decoding means for decoding the protected data on the basis of the protection format information and generating the data of a printable format, a storage means for protecting the data of the printable format in accordance with the protection format and storing the protected data in a storage device, and an output means for decoding the protected data stored in the storage device in accordance with an operator's instruction and outputting printable data to a printer.

## LEGAL STATUS

[Date of request for examination]

02.12.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2001-117744  
(P2001-117744A)

(43) 公開日 平成13年4月27日 (2001. 4. 27)

(51) IntCl <sup>7</sup>	識別記号	F I	テマコード* (参考)
G 0 6 F 3/12		G 0 6 F 3/12	K 2 C 0 6 1
			D 5 B 0 2 1
B 4 1 J 29/38		B 4 1 J 29/38	Z 5 B 0 8 9
G 0 6 F 13/00	3 5 1	G 0 6 F 13/00	3 5 1 Z

審査請求 未請求 請求項の数10 O L (全 25 頁)

(21) 出願番号 特願平11-294452

(22) 出願日 平成11年10月15日 (1999. 10. 15)

(71) 出願人 000001007

キヤノン株式会社

東京都大田区下丸子3丁目30番2号

(72) 発明者 佐藤 真之

東京都大田区下丸子3丁目30番2号 キヤ  
ノン株式会社内

(72) 発明者 下野 雅樹

東京都大田区下丸子3丁目30番2号 キヤ  
ノン株式会社内

(74) 代理人 100090273

弁理士 國分 孝悦

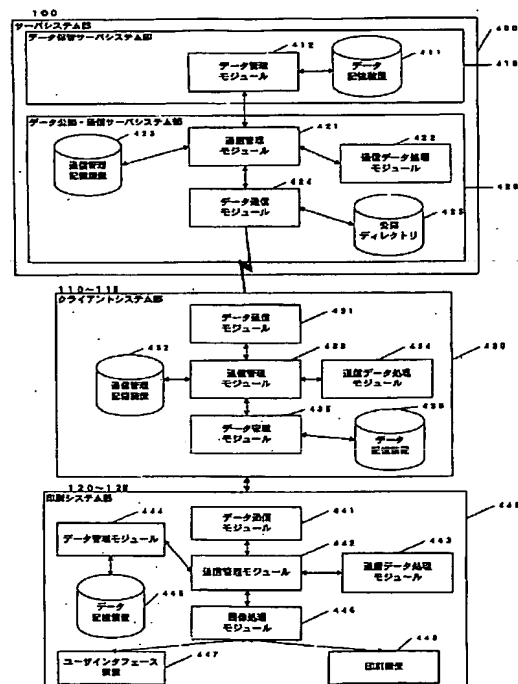
最終頁に続く

(54) 【発明の名称】 印刷システム、印刷方法及び記録媒体

(57) 【要約】

【課題】 入力されたデータを印刷するまで保護することが  
できる印刷システムを提供することを課題とする。

【解決手段】 本発明の印刷システムは、保護されたデータ  
と該保護データの保護形式の情報を入力する入力手段  
と、該保護形式の情報に基づいて保護データを復号化し、  
印刷可能な形式のデータを生成する復号化手段と、  
印刷可能な形式のデータを上記の保護形式に従ってデータ  
保護し、記憶装置内に保管する保管手段と、オペレー  
タの指示により記憶装置内に保管された保護データを復  
号化し、印刷可能になったデータを印刷装置に出力する  
出力手段とを有する。



## 【特許請求の範囲】

【請求項1】 保護されたデータと該保護データの保護形式の情報を入力する入力手段と、  
該保護形式の情報に基づいて該保護データを復号化し、印刷可能な形式のデータを生成する復号化手段と、  
該印刷可能な形式のデータを前記保護形式に従ってデータ保護し、記憶装置内に保管する保管手段とを有する印刷システム。

【請求項2】 さらに、前記記憶装置内に保管された保護データを復号化し、印刷可能になったデータを印刷装置に出力する出力手段を有する請求項1記載の印刷システム。

【請求項3】 前記出力手段は、オペレータの指示により前記保護データを復号化して印刷装置に出力する請求項2記載の印刷システム。

【請求項4】 さらに、前記出力手段が出力するデータを印刷する印刷装置を有する請求項2又は3記載の印刷システム。

【請求項5】 前記出力装置は、さらに、復号化したデータを表示装置に出力する請求項2～4のいずれかに記載の印刷システム。

【請求項6】 さらに、前記出力手段が出力するデータを表示する表示装置を有する請求項5記載の印刷システム。

【請求項7】 前記データ保護形式は、1つ以上のデータ暗号化形式から選択された一つのデータ暗号化形式、又は可視透かしデータ付与、又は不可視透かしデータ付与、のうちの1つ又は2つ以上の組み合わせである請求項1～6のいずれかに記載の印刷システム。

【請求項8】 前記入力手段は、ネットワークを介して入力する請求項1～7のいずれかに記載の印刷システム。

【請求項9】 (a) 保護されたデータと該保護データの保護形式の情報を入力するステップと、

(b) 該保護形式の情報に基づいて該保護データを復号化し、印刷可能な形式のデータを生成するステップと、

(c) 該印刷可能な形式のデータを前記保護形式に従ってデータ保護し、記憶装置内に保管するステップとを有する印刷方法。

【請求項10】 (a) 保護されたデータと該保護データの保護形式の情報を入力する手順と、

(b) 該保護形式の情報に基づいて該保護データを復号化し、印刷可能な形式のデータを生成する手順と、

(c) 該印刷可能な形式のデータを前記保護形式に従ってデータ保護し、記憶装置内に保管する手順とをコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】 本発明は、印刷技術に関し、

特に印刷データを保護するための印刷技術に関する。

## 【0002】

【従来の技術】 クライアント／サーバ型分散処理システムでは、データの転送時にインターネット上の一般的な通信手段を使用する場合がある。その場合、データを公開ディレクトリに置くか、または公開された手順に従って処理要求をおこなう方法が一般的である。従来の技術では、データを保護しようとする場合、通信回線上の信号を暗号化するか、あらかじめ暗号化されたデータを公開ディレクトリに置いて、受信者が復号鍵で明示的にデータを復号化する方法が一般的である。また、特に画像データなどは情報量が非常に多くなるため、復号化の処理などに大きな負荷がかかっていた。さらに、受信後に復号化した画像などのデータを保護する手段は提供されていなかった。

## 【0003】

【発明が解決しようとする課題】 従来技術では、公開されたディレクトリ上に置かれたデータそのものは保護されない。また、受信者が復号鍵で明示的にデータの復号化を行わなければならない、受信者の処理負荷が大きくなるといった問題があった。

【0004】 また、受信者が先の画像データなどを取得し、一度、明示的に復号化した後の画像データは保護することが出来ないといった問題があった。

【0005】 本発明の目的は、入力されたデータを印刷するまで保護することができる印刷システム、印刷方法及び記録媒体を提供することである。

## 【0006】

【課題を解決するための手段】 本発明の一観点によれば、保護されたデータと該保護データの保護形式の情報を入力する入力手段と、該保護形式の情報に基づいて該保護データを復号化し、印刷可能な形式のデータを生成する復号化手段と、該印刷可能な形式のデータを前記保護形式に従ってデータ保護し、記憶装置内に保管する保管手段とを有する印刷システムが提供される。

【0007】 本発明の他の観点によれば、(a) 保護されたデータと該保護データの保護形式の情報を入力するステップと、(b) 該保護形式の情報に基づいて該保護データを復号化し、印刷可能な形式のデータを生成するステップと、(c) 該印刷可能な形式のデータを前記保護形式に従ってデータ保護し、記憶装置内に保管するステップとを有する印刷方法が提供される。

【0008】 本発明のさらに他の観点によれば、(a) 保護されたデータと該保護データの保護形式の情報を入力する手順と、(b) 該保護形式の情報に基づいて該保護データを復号化し、印刷可能な形式のデータを生成する手順と、(c) 該印刷可能な形式のデータを前記保護形式に従ってデータ保護し、記憶装置内に保管する手順とをコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体が提供され

る。

【0009】本発明によれば、データを保護して記憶装置内に保管することにより、データを入力してから印刷されるまでの間、印刷データを保護することができる。また、印刷処理などの前処理の負荷を軽減することができる。

【0010】

【発明の実施の形態】以下、本発明の実施形態を図面に基づいて説明する。

＜ネットワークシステム構成＞図1は、本発明の実施例によるネットワークシステム全体の構成図である。図1中100は情報処理装置（ネットワーク機器）である。情報処理装置100は、図2において後述するCPU、ROM、RAM、HDDなどから構成されるコンピュータシステムである。以下、情報処理装置100をサーバコンピュータという。

【0011】サーバコンピュータ100は、後述するクライアントコンピュータ110～11N（Nは整数）からの要求に基づいて、クライアントコンピュータ110～11Nに伝送するための情報や画像などのデータを保持し、データの加工などをする機能を有し、さらに、クライアントコンピュータ110～11Nからの要求に基づいて、データを収集し、公開ディレクトリに設置し、管理する機能を有する。

【0012】110～11Nは情報処理装置（ネットワーク機器）である。情報処理装置110～11Nは、図2において後述するCPU、ROM、RAM、HDDなどから構成されるコンピュータシステムである。以下、情報処理装置110～11Nをクライアントコンピュータという。

【0013】クライアントコンピュータ110～11Nは、ネットワーク130を通してサーバコンピュータ100に格納されている例えば画像などのデータを公開ディレクトリから取得する機能と、データを加工する機能とを有し、さらに、後述する印刷システム120～12Nに対してデータを印刷する指示を行う機能とを有する。

【0014】120～12Nは、クライアントコンピュータ110～11Nからの印刷指示に基づいて画像を印刷する機能と、データを加工する機能とを持つ情報処理装置である。以下、情報処理装置120～12Nを印刷システムという。

【0015】130は、クライアントコンピュータ110～11Nとサーバコンピュータ100を接続する接続装置である。接続装置130は、例えばローカルエリアネットワーク（LAN）やインターネットなどのネットワークシステムを表すものである。以下、接続装置130をネットワークという。

【0016】なお、本実施例においては、ネットワーク130は一般的なインターネットの場合を説明するが、

その他のネットワークを使用しても実現可能である。また、クライアントコンピュータ110～11N、サーバコンピュータ100、及び印刷システム120～12Nなどのいくつかは、物理的に同一のコンピュータで兼用することも可能である。

【0017】＜クライアントコンピュータ、サーバコンピュータのブロック図＞図2は、本発明の一実施例によるクライアントコンピュータ110～11N及びサーバコンピュータ100のシステム構成を示すブロック図である。本実施例では、クライアントコンピュータ110～11N及びサーバコンピュータ100の内部構成については差異がないため、図2で一括してハードウェア構成の説明を行う。以下、クライアントコンピュータ110～11N及びサーバコンピュータ100を総称して、情報処理装置という。

【0018】図2中201は情報処理装置の制御をつかさどる中央演算装置（以下CPUと記す）である。202はランダムアクセスメモリ（以下RAMと記す）であり、CPU201の主メモリとして、及び実行プログラム（コンピュータプログラム）の記憶領域や該プログラムの実行エリアならびにデータエリアとして機能する。

【0019】203はCPU201の動作処理手順を記憶しているリードオンリーメモリ（以下ROMと記す）である。ROM203は、情報処理装置の機器制御を行うシステムプログラムである基本ソフト（OS）を記録したプログラムROMと、システムを稼働するために必要な情報等が記録されたデータROMを有する。ROM203の代わりに、後述のハードディスクドライブ（HDD）209を用いる場合もある。

【0020】204はネットワークインターフェース（NETIF）であり、ネットワークを介して情報処理装置間のデータ転送を行うための制御や接続状況の診断を行う。205はビデオRAM（VRAM）であり、情報処理装置の稼働状態を示す後述する表示装置（CRT）206の画面に表示される画像データを展開し、その表示の制御を行う。

【0021】206は表示装置であって、例えばディスプレイなどである。以下、表示装置206をCRTと記す。207は後述する外部入力装置（KB）208からの入力信号を制御するためのコントローラ（KBC）である。

【0022】208は情報処理装置の利用者（ユーザ）が情報処理装置に対して行う操作を受けつけるための外部入力装置であり、例えばキーボードや、マウスなどのポインティングデバイスである。以下、外部入力装置208をKBと記す。209はハードディスクドライブ（HDD）であり、アプリケーションプログラムや、画像情報などのデータ保存用に用いられる。本実施例におけるアプリケーションプログラムとは、本実施例を構成する各種処理手段を実行するソフトウェアプログラムな

どである。

【0023】210は外部入出力装置であって、例えばフロッピーディスクドライブ、CD-ROMドライブなどのリムーバブルディスクを入出力することができるものであり、上述したアプリケーションプログラムを記録媒体から読み出す際に用いられる。以下、外部入出力装置210をFDDと記す。

【0024】なお、HDD209に格納するアプリケーションプログラムやデータをFDD210に格納して使用することも可能である。200は上述した各ユニット間を接続するための入出力バス（アドレスバス、データバス、及び制御バス）である。

【0025】＜印刷システムのブロック図＞図3は本実施例による印刷システム120～12Nのシステム構成を示すブロック図である。図3中301は印刷システムである情報処理装置を制御するCPUである。302はRAMであり、CPU301の主メモリとして、及び実行プログラムの格納領域や該プログラムの実行エリアならびにデータエリアとして機能する。

【0026】303はCPU301の動作処理手順を記憶しているROMである。ROM303は、プリントサーバ（例えばクライアントコンピュータ110～11N）の機器制御を行うシステムプログラムである基本ソフト（OS）を記録したプログラムROMと、システムを稼働するために必要な情報等が記録されたデータROMを有する。ROM303の代わりに、後述のHDD309を用いる場合もある。

【0027】304はネットワークインターフェース（NETIF）であり、ネットワークを介してサーバコンピュータ100など他の情報処理装置とのデータ転送を行うための制御や接続状況の診断を行う。305はVRAMであり、プリントサーバである情報処理装置の稼働状態を示す後述するCRT306の画面に表示される画像データを展開し、その表示の制御を行う。

【0028】306は表示装置であって、例えばディスプレイなどである。以下、表示装置306をCRTと記す。307は後述する外部入力装置308からの入力信号を制御するためのコントローラ（KBC）である。

【0029】308は情報処理装置の利用者が情報処理装置に対して行う操作を受けつけるための外部入力装置であり、例えばキーボードや、マウスなどのポインティングデバイスである。以下、外部入力装置308をKBと記す。309はハードディスクドライブ（HDD）であり、印刷を制御するアプリケーションプログラムや、画像情報などのデータ保存用に用いられる。

【0030】310は外部入出力装置であって、例えばフロッピーディスクドライブ、CD-ROMドライブなどのリムーバブルディスクを入出力することができるものであり、上述したアプリケーションプログラムの記録媒体から読み出す際に用いられる。以下、外部入出力装

置310をFDDと記す。

【0031】なお、HDD309に格納するアプリケーションプログラムやデータをFDD310に格納して使用することも可能である。311はプリンタ制御装置であって、後述する外部出力装置312の制御と出力する画像データの制御を行う。以下、プリンタ制御装置311をPRTCと記す。

【0032】312は外部出力装置であって、例えばプリンタである。以下、外部出力装置312をPRTと記す。313は拡張外部入出力装置制御装置であり、後述する拡張外部入出力装置314を制御する。以下、拡張外部入出力装置制御装置313をCTLRと記す。

【0033】314は拡張外部入出力装置であり、例えばイメージスキャナのように印刷物を読み取るなど、画像データの外部入力機能を持つ装置である。300は上述した各ユニット間を接続するための入出力バス（アドレスバス、データバス、及び制御バス）である。

【0034】＜ネットワークシステムのモジュール構成＞図4は、本実施例によるネットワークシステムのモジュール構成図である。図1のサーバコンピュータ100は、図4のサーバシステム部400に相当する。サーバシステム部400は、データ保管サーバシステム部410とデータ公開・通信サーバシステム部420を有する。

【0035】データ保管サーバシステム部410は、データ管理モジュール412とデータ記憶装置411を有する。データ公開・通信サーバシステム部420は、通信管理モジュール421、通信データ処理モジュール422、通信管理記憶装置423、データ通信モジュール424および公開ディレクトリ425を有する。

【0036】データ記憶装置411は、画像や画像情報などのデータを格納するテーブルを有し、検索可能な状態でデータをHDD209（図2）内に格納する装置である。データ管理モジュール412は、データ記憶装置411のデータを管理する機能と、データ内容を解釈、判断し、適当な処理を行う機能と、要求されたデータをデータ記憶装置411から取り出し、後述するデータ属性情報とともに通信管理モジュール421に引き渡す機能とを有する。

【0037】通信管理モジュール421は、データ通信モジュール424から後述するセキュリティ情報と要求されたデータの内容を取得する機能と、データ通信モジュール424から後述するセキュリティ情報とクライアントシステム部430から送付されるデータ内容を取得する機能と、通信管理記憶装置423に保管された後述する通信データを更新する機能とを有する。

【0038】通信データ処理モジュール422は、データの暗号化、データ圧縮、複数データの結合、単一データの分解といったデータの加工を行う機能を有する。通信管理記憶装置423は、後述する送信データテーブル

とセキュリティ管理テーブルを有し、検索可能な状態でデータをHDD209（図2）内に格納する装置である。

【0039】データ通信モジュール424は、ネットワークを介してデータの送受信を行うことができる機能を有し、通信管理モジュール421から引き渡されたデータを指定された公開ディレクトリ425に保管する機能と公開ディレクトリ425上の公開データを削除する機能を有する。

【0040】図1のクライアントコンピュータ110～11Nは、図4のクライアントシステム部430に相当する。クライアントシステム部430は、データ通信モジュール431、通信管理記憶装置432、通信管理モジュール433、通信データ処理モジュール434、データ管理モジュール435およびデータ記憶装置436を有する。

【0041】データ通信モジュール431は、ネットワークを介してデータの送受信を行うことができる機能を有する。通信管理記憶装置432は、先の通信管理記憶装置423と同様である。通信管理モジュール433は、通知された公開ディレクトリ425の場所、通信データサイズ、通信データ情報、セキュリティ情報などを取得し、通信時間とともに通信管理記憶装置432に保管する機能と、データ管理モジュール435を介してデータ記憶装置436から後述する通信データを取得する機能を有する。

【0042】通信データ処理モジュール434は、通信データ処理モジュール422と同様の機能を有する。データ管理モジュール435は、データ記憶装置436のデータを管理する機能と、データ内容を解釈、判断し、適切な処理を行う機能と、要求されたデータをデータ記憶装置436から取り出し、後述するデータ属性情報とともに通信管理モジュール433に引き渡す機能とを有する。

【0043】データ記憶装置436は、画像や画像情報などのデータを格納するテーブルを有し、検索可能な状態でデータをHDD209（図2）内に格納する装置である。図1の印刷システム120～12Nは、図4の印刷システム部440に相当する。印刷システム部440は、データ通信モジュール441、通信管理モジュール442、通信データ処理モジュール443、データ管理モジュール444、データ記憶装置445、画像処理モジュール446、ユーザインタフェース装置447および印刷装置448を有する。

【0044】データ管理モジュール444、通信管理モジュール442、及び通信データ処理モジュール443は、各々、クライアントシステム部430のデータ管理モジュール435、通信管理モジュール433、及び通信データ処理モジュール434と同様の機能を有する。

【0045】画像処理モジュール446は、印刷時の対

象画像に対して画像処理をする機能を有する。ユーザインタフェース装置447は、印刷依頼の対象になる画像およびファイルの枚数、形式などの選択等の一部または全部を操作する画面を表示する表示装置及び入力装置である。

【0046】印刷装置448は、例えばレーザビーム方式でカラー可視画像を形成（印刷）する。なお、記録方式はレーザビーム方式に限られるものではなく、熱転写方式やインクジェット方式等いかなるものでもよい。通信データ処理モジュール443は、暗号化および復号化が必要なファイルを暗号化・復号化処理する機能と、透かし（電子透かし）データ付加・削除処理が必要なファイルに透かしデータの付加・削除する処理の機能を有する。

【0047】データ記憶装置445は、図2のハードディスクドライブ309又はリムーバブルディスクドライブ310に相当し、画像データ等について容易に検索、更新、追加、削除をすることができる。図4中412、421、422、424、431、433、434、435、441、442、443、444、446の各モジュールは、アプリケーションプログラムにより実現され、ROM203、HDD209またはFDD210より読み込まれ、RAM202に展開されて使用される。411、423、425、432、436及び445は、HDD209内に格納されるデータである。

【0048】＜動作説明＞図4を用いて本実施例の全体的な動作説明を行う。はじめにクライアントシステム部430からの要求に基づいて、データをサーバシステム部400からクライアントシステム部430に送付する場合の処理の流れについて説明する。

【0049】クライアントシステム部430は、クライアントシステム部430の通信管理記憶装置432に保管された通信情報に基づいて、セキュリティ情報の送信とともにデータの要求を行う通信を、データ公開・通信サーバシステム部420に対して行う。通信は、クライアントシステム部430のデータ通信モジュール431からデータ公開・通信サーバシステム部420のデータ通信モジュール424に対して行われる。

【0050】セキュリティ情報には、利用者を特定する識別子（ID）とパスワード、要求されるセキュリティの強さ、あるいはそれらの一部、または全てが含まれる。セキュリティ情報についての詳細は後述する。データ公開・通信サーバシステム部420のデータ通信モジュール424は、クライアントシステム部430からの通信内容を取得したことをデータ公開・通信サーバシステム部420の通信管理モジュール421に通知する。

【0051】図5は、サーバシステム部400の処理を示すフローチャートである。まず、ステップS501では、通信管理モジュール421がデータ通信モジュール424から先のセキュリティ情報と要求されたデータの

内容を取得する。次に、ステップS502では、通信管理モジュール421が、取得した情報に先のセキュリティ情報が含まれていないか否かを判断する。セキュリティ情報が含まれていない場合には、ステップS503へ進む。ステップS503では、要求されたデータが一般に公開する事が可能なデータであるかどうかを通信管理記憶装置423に保管された先のセキュリティ情報と照合して判断する。

【0052】一般に公開可能なデータでなければ、ステップS511へ進み、処理を終了する。一般に公開可能なデータであれば、ステップS506へ進む。ステップS506では、データ管理モジュール412にデータを要求し、取得する。ステップS502で先のセキュリティ情報が含まれていると判断された場合には、ステップS504へ進む。ステップS504では、要求されたデータがそのセキュリティ情報で公開することが可能なデータであるかどうかを通信管理記憶装置423に保管されているセキュリティ情報と照合し、ステップS505へ進む。ステップS505では、照合の結果、一般に公開する事が可能なデータであるか否かを判断する。

【0053】公開可能でなければ、ステップS511へ進み、処理を終了する。公開可能であれば、ステップS506へ進む。ステップS506では、データ管理モジュール412にデータを要求し、取得する。ステップS506の処理を詳述する。ステップS506では、データ管理モジュール412が、要求されたデータをデータ記憶装置411から取り出し、データ属性情報とともに通信管理モジュール421に引き渡す。ここに要求されたデータは、一つのデータファイルである場合と複数のデータファイルから構成される場合がある。

【0054】ステップS506の後、ステップS507では、通信管理モジュール421が、取得していた先のセキュリティ情報とデータ管理モジュール412から取得したデータの属性情報を基に、データの処理を通信データ処理モジュール422に依頼する。ここでデータ処理とは、データの暗号化、データ圧縮、複数データの結合、単一データの分解といったデータの加工を意味する。

【0055】次に、ステップS508では、通信管理モジュール421が、通信データ処理モジュール422により処理されたデータをデータ通信モジュール424に引き渡す。この時、データの要求を行った利用者を特定する情報が先のセキュリティ情報に含まれていた場合、実際に要求を行ったクライアントシステム部430から参照できる公開ディレクトリ425を指定する。また、同時にデータを特定する情報、データ管理モジュール412からデータを取得した時間、利用者を特定する情報、データの処理内容、特定のセキュリティ情報などを通信管理記憶装置423に保管する。なお、このデータ通信モジュール424への引き渡しに関しては、通信デ

ータサイズを考慮する。

【0056】次に、ステップS509では、データ通信モジュール424が、通信管理モジュール421より引き渡されたデータを指定された公開ディレクトリ425に保管する。次に、ステップS510では、上記の保管が完了した後に、クライアントシステム部430のデータ通信モジュール431に対して、データの準備が完了したことを、保管した公開ディレクトリ425の場所、通信データサイズ、通信データ情報、セキュリティ情報などとともに通知する。その後、ステップS511へ進み、処理を終了する。

【0057】図6は、上述の図5のフローチャートの処理の後、通知を受けたクライアントシステム部430が行う処理の流れを示すフローチャートである。まず、ステップS601では、クライアントシステム部430が、サーバシステム部400からデータ通信モジュール431に対して行われた通知を取得する。データ通信モジュール431は、通信管理モジュール433に、データの準備が完了した通知を受けたことを通知する。

【0058】次に、ステップS602では、通信管理モジュール433が、通知された公開ディレクトリ425の場所、通信データサイズ、通信データ情報、セキュリティ情報などを取得し、通信時間とともに通信管理記憶装置432に保管する。次に、ステップS603では、通信管理モジュール433が、続いてデータを受信するようにデータ通信モジュール431に要求する。なお、この受信の要求に関しては通信データサイズなどを考慮する。データ通信モジュール431は、通知された公開ディレクトリ425の情報に基づいて、サーバシステム部400のデータ通信モジュール424を介して、公開ディレクトリ425よりデータを取得する。データを取得した際には、データの準備が完了したことを示す通知とともに受け取った先の通信データ情報を考慮する。データの取得が完了した場合、データ通信モジュール431はその正否を含めた完了情報を通信管理モジュール433に通知する。

【0059】次に、ステップS604では、通信管理モジュール433が、先に通信管理記憶装置432に保管した通信データ情報やセキュリティ情報に従って、通信データ処理モジュール434に、取得したデータの処理を依頼する。ここでデータ処理とは、データの復号化、データの伸張、複数データへの分解、単一データへの結合といったデータの加工を意味する。

【0060】次に、ステップS605では、通信管理モジュール433が、通信データ処理モジュール434により処理されたデータをデータ管理モジュール435に引き渡す。データ管理モジュール435は、引き渡されたデータをデータ記憶装置436に格納する。

【0061】この時、データ管理モジュール435にデータ内容を解釈、判断し、適当な処理を行う処理動作が

記述されていれば、たとえば、印刷システム部440のデータ通信モジュール441にデータの格納を通知し、ユーザインターフェイス装置442から画像処理モジュール441を介してデータを取得し、印刷装置443に出力を行ったり、ユーザインターフェイス装置442に表示せず直接印刷装置443に出力可能である。

【0062】次に、ステップS606では、通信管理モジュール433が、正しく先の通信データを受け取れたか否かを判断し、正しく受け取れた場合には、通信管理モジュール433が、データ通信モジュール431に対し、データの取得が完了したことをデータ公開・通信サーバシステム部420に通知するよう依頼する。その後、処理を終了する。

【0063】図7は、上述の図6のフローチャートの処理の後、通知を受けたサーバシステム部400が行う処理の流れを示すフローチャートである。まず、ステップS701では、データ公開・通信サーバシステム部420のデータ通信モジュール424が、クライアントシステム部430からデータの取得が完了したことの通知を受け取った場合、この通知をデータ公開・通信サーバシステム部420の通信管理モジュール421に報告する。

【0064】次に、ステップS702では、通信管理モジュール421が、通信管理記憶装置423に保管された通信データを、完了日時などを基に更新する。次に、ステップS703では、通信管理モジュール421が、公開ディレクトリ425上に公開された通信データが必要であり、削除する必要があるか否かを判断する。削除する必要がないと判断された場合には、処理を終了する。削除する必要があると判断された場合には、ステップS704へ進む。

【0065】この判断は、通信管理記憶装置423に保管された後述する通信管理情報などにしたがって、公開時間やセキュリティのレベル、同時あるいは連続して行われているその他のデータ要求などに従って行われる。ステップS704では、通信管理モジュール421が、データ通信モジュール424に対して、公開ディレクトリ425上の公開データを削除するよう依頼する。データ通信モジュール424は、先の公開データを削除する要求を受けた場合に、公開された該当データを削除する。その後、処理を終了する。

【0066】このフローチャートの処理は、クライアントシステム部430がサーバシステム部400上のデータを必要とする任意のタイミングで行うことができる。また、クライアントシステム部430が設定された一定の時間間隔をおいてデータ要求を行っても良い。

【0067】次に、クライアントシステム部430の要求に基づいて、データをクライアントシステム部430からサーバシステム部400に送付する場合の処理の流れについて説明する。最初に行われる処理は、先に説明

したデータをサーバシステム部400からクライアントシステム部430に送付する場合の処理の流れと同様である。サーバシステム部400は、先のセキュリティ情報をクライアントシステム部430から受け取って、データ公開・通信サーバシステム部420のデータ通信モジュール424に通知する。

【0068】図8は、サーバシステム部400の処理を示すフローチャートである。まず、ステップS801では、通信管理モジュール421が、データ通信モジュール424から先のセキュリティ情報とクライアントシステム部430より送付されるデータ内容情報を取得する。次に、ステップS802では、通信管理モジュール421は受け取った情報が適切(適当)であるか否かを判断する。適切でないと判断される場合には、処理を終了する。適切であると判断される場合には、ステップS803へ進む。

【0069】ステップS803では、通信管理モジュール421が、データ通信モジュール424に対して公開ディレクトリ425の割り当てを要求する。次に、ステップS804では、通信管理モジュール421が、上記の取得した情報を通信管理記憶装置423に保管する。

【0070】次に、ステップS805では、上記の処理が完了した後、通信管理モジュール421が、データ通信モジュール424に対しクライアントシステム部430に準備が完了したことを通知するよう依頼する。データ通信モジュール424は、この依頼を受けて、公開ディレクトリ名などを、クライアントシステム部430のデータ通信モジュール431に通知する。その後、処理を終了する。

【0071】図9は、上述の処理の後、準備が完了した旨の通知を受けたクライアントシステム部430が行う処理の流れを示すフローチャートである。まず、ステップS901では、データ通信モジュール431が、通信管理モジュール433に取得した公開ディレクトリ名などとともにサーバシステム部400の準備が完了したことを報告する。

【0072】次に、ステップS902では、通信管理モジュール433が、公開ディレクトリ名などの取得情報を通信管理記憶装置432に格納する。次に、ステップS903では、通信管理モジュール433が、データ管理モジュール435を介してデータ記憶装置436から通信データを取得する。

【0073】次に、ステップS904では、通信管理モジュール433が、通信データ処理モジュール434に依頼して、取得した通信データの処理を行わせる。ここで、データの処理とは、データの復号化、データの伸張、複数データへの分解、単一データへの結合といったデータの加工を意味し、データの属性やセキュリティのレベルによって処理が行われる。

【0074】次に、ステップS905では、処理が完了



すると、通信管理モジュール433が、データ通信モジュール431を介してデータをサーバシステム部400に送信する。送信が完了すると、完了したことがサーバシステム部400に通知される。

【0075】この後、サーバシステム部400では、データ送信が完了した旨の通知を受け取ると、データをサーバシステム部400からクライアントシステム部430に送付する場合のクライアントシステム部430の処理の流れと同様に、データ処理を行ってデータ記憶装置411にデータを格納する。ただし、この場合には、データ記憶装置411にデータが格納された後に、公開ディレクトリ425上のデータは削除される。

【0076】＜通信データ構成および送受信データテーブルとセキュリティ管理テーブル＞クライアントシステム部430とサーバシステム部400との間で通信を行う場合において、使用される通信データ群、および通信管理記憶装置423、432に記憶される送信データテーブルとセキュリティ管理テーブルについて説明する。

【0077】図10は、通信データ群の一部を示したものである。通信データ群は、利用者を特定する識別子（ID）1000、パスワード1001、アクセストークンまたはアクセストークンシード1002、要求内容1003、セキュリティの強さ1004、アプリケーションデータ1005の6つの項目を有する。通信データは、常にすべての項目を有する必要はない。また、要求内容1003とアプリケーションデータ1005は、場面に応じて意味が異なっている場合がある。

【0078】たとえば、クライアントシステム部430からサーバシステム部400にデータを要求する際には、要求内容1003は、要求するデータそのものであり、アプリケーションデータ1005にはそれに付随する情報が含まれる。この場合、要求されるデータは2種類のデータタイプと2種類の要求タイプから構成されている。

【0079】データタイプには、利用者を特定するID1000に対応するデータ群を指定する「送信待ちデータ（w）」と、特定の利用者に対応していない「一般データ（g）」との2種類がある。要求タイプには、データそのものを要求する「データ要求（r）」と、該当データのサイズを要求する「サイズ要求（s）」との2種類がある。

【0080】送信待ちデータ（w）が指定されている場合には、アプリケーションデータ1005には最大受信量といった情報が含まれ、一般データ（g）が指定されている場合には、アプリケーションデータ1005には、要求する具体的なファイル名を特定する情報などが含まれる場合がある。

【0081】クライアントシステム部430がデータを受信し、通信が完了したことを確認する通知をサーバシステム部400に送付する場合には、要求内容1003

には「受信完了（rc）」が設定される。

【0082】図11は、送受信データテーブルの構成の一部を示したものである。送受信データテーブル1100は、ID1101、送受信ステータス1102、ファイル名特定情報1103、セキュリティの強さ1104、ファイル形式1105、データ通信構成情報1106を有する。

【0083】セキュリティの強さ1104、及びファイル形式1105は、必ずしも設定されない場合がある。

ID1101は、クライアントシステム部430から前述のセキュリティ情報の一部として送付される利用者を特定するIDと等価な情報である。送受信ステータス1102には、おおまかに、送受信待ち、送受信中、送受信完了といったステータスが設定される。

【0084】図12は、セキュリティ管理テーブルの構成の一部を示したものである。セキュリティ管理テーブル1200は、ID1201、パスワード1202、アクセストークン1203、セキュリティの強さ1204、及び要求日時1205を有する。これらの項目は、クライアントシステム部430から前述のセキュリティ情報として送付する場合に使用される情報である。

【0085】＜セキュリティ処理＞本実施例の特徴の一つである、データ公開・通信サーバシステム部420の通信管理モジュール421が行うセキュリティに関する処理の詳細について説明する。

【0086】クライアントシステム部430からサーバシステム部400にデータを要求する場合にも、クライアントシステム部430からサーバシステム部400にデータを送信する場合にも、まず最初に先で述べたセキュリティ情報が送信される。セキュリティ情報には、前述の利用者を特定するIDとパスワード、要求されるセキュリティの強さ、あるいは、それらの一部、または全てが含まれる。

【0087】はじめに、先の利用者を特定するIDとパスワードを、通信管理記憶装置423に格納されている前述のセキュリティ管理テーブル1200に保管されたID1201とパスワード1202を照合する。一致しない場合には、本処理の特定の条件を満たす場合を除いて継続されない。特定の条件とは、要求するデータがセキュリティを必要としない場合などであり、この詳細については後述する。

【0088】次に、通信管理モジュール421は、ランダムな文字列または数値を発生させ、クライアントシステム部430に通知するとともに、この発生させたデータにある特定の演算を適用して作成された文字列または数値を通信管理記憶装置423にある前述のセキュリティ管理テーブル1200に保管する。

【0089】本実施例では、ランダムに発生させた先のデータ、文字列または数値を「アクセストークンシード」、これを演算して得られる結果を「アクセストーク

ン」と呼ぶ。クライアントシステム部430に通知されるデータには、アクセストークンシードが含まれる。なお、アクセストークンおよびアクセストークンシードに関する処理は、通信のたびに利用者を特定するIDとパスワードが送付される場合は不要である。たとえば、サーバシステム部400が公開ディレクトリ425にデータを公開し、クライアントシステム部430がこれを取得した際に、取得を完了したことをサーバシステム部400に通知する場合、前述の利用者を特定するIDとパスワードが送付されるならば、アクセストークンに関する処理は不要となる。

【0090】また、クライアントシステム部430へのアクセストークンシードの通知は、サーバシステム部400が公開ディレクトリ425にデータを公開したことを通知する場合や、クライアントシステム部430からのデータ送付を行う公開ディレクトリ425を用意できたことを通知する場合に同時に送付される。

【0091】クライアントシステム部430の通信管理モジュール433は、サーバシステム部400から送付されたアクセストークンシードを通信管理記憶装置432のセキュリティ管理テーブル1200に保管する。この保管されたアクセストークンシードは、サーバシステム部400とこれ以上の通信が不要となるまで利用される。次の通信の際に利用者を特定するIDとパスワードを送付する代わりにアクセストークンを使用する場合には、サーバシステム部400と同じ特定の演算を適用して作成された文字列または数値をアクセストークンとする。

【0092】ここで、クライアントシステム部430から、サーバシステム部400にデータを要求する場合について図13を用いて説明する。図13は、データ公開・通信サーバシステム部420の通信管理モジュール421がクライアントシステム部430からデータを要求された場合のサーバシステム部400のセキュリティに関連する処理を示すフローチャートである。

【0093】まず、ステップS1301では、通信管理モジュール421が、取得した情報（セキュリティ情報）にIDが含まれているかどうかを判断する。IDが含まれていなければ、ステップS1303へ進む。IDが含まれている場合であっても、パスワードとともにIDが正しいかどうか通信管理記憶装置423の情報と照合し、照合した結果、正しいセキュリティ情報でないと判断された場合にも、ステップS1303へ進む。ステップS1303において、取得した情報にアクセストークンが含まれていないと判断された場合には、ステップS1302へ進む。

【0094】ステップS1302では、照合（照会）した結果、正しいセキュリティ情報でないと判断された場合、あるいはセキュリティ情報が含まれていない場合には、取得したセキュリティ情報とともに処理日時などを

記録して、セキュリティエラーフラグを記録する。その後、処理を終了する。

【0095】ステップS1303において、取得した情報にセキュリティ情報ではなくアクセストークンが含まれていた場合には、ステップS1304へ進む。ステップS1304では、アクセストークンを基にセキュリティ管理テーブル1200を検索し、IDを取得する。IDが存在しないか又はIDが正しくない場合には、ステップS1302へ進み、上記と同様の処理を行う。IDが正しい場合には、ステップS1305へ進む。

【0096】また、ステップS1301において、取得したセキュリティ情報にIDが含まれており、そのIDがパスワードとともに正しいかどうか通信管理記憶装置423の情報と照合し、照合した結果、正しいセキュリティ情報であると判断された場合にも、ステップS1305へ進む。

【0097】ステップS1305では、アクセストークンシードの生成を行って、これを一時記憶領域に保管する。次に、ステップS1306では、アクセストークンシードを基にアクセストークンを生成し、要求されたデータや処理日時とともに通信管理記憶装置423に記録する。

【0098】次に、ステップS1307では、要求されたデータの種類（データタイプ）について判断を行う。要求されるデータの種類の種類が「一般データ（g）」の場合には、セキュリティエラーフラグが記録されていた場合でも処理が継続される。「送信待ちデータ（w）」の場合には、セキュリティエラーフラグが記録されていた場合に、ステップS1308で要求拒否をクライアントシステム部430に通知する。

【0099】次に、ステップS1309では、要求されるデータの種類の種類が「一般データ（g）」の場合には、さらに通信データ群のアプリケーションデータ1005（図10）内に指定された具体的なファイル名を特定する情報から、要求データが存在するかどうかを判断する。

【0100】存在しない場合には、ステップS1310へ進み、要求のエラーをクライアントシステム部430に通知する。その後、処理を終了する。存在する場合には、ステップS1311へ進む。ステップS1311では、要求されるデータの種類の種類が「送信待ちデータ

（w）」の場合には、IDに対応したクライアントシステム部430が受信していないデータが存在するかどうかを通信管理記憶装置423の送受信データテーブル1100と照合（照会）して判断する。未受信データが存在すれば、ステップS1310へ進み、該当するデータが存在しないことをクライアントシステム部430にエラーとして通知し、処理を終了する。未受信データが存在しなければ、ステップS1312へ進む。

【0101】ステップS1312では、要求されるデー

タの要求種類（要求タイプ）が「サイズ要求（s）」であるか否かを判断する。「サイズ要求（s）」である場合には、ステップS 1313へ進み、対象となるデータのサイズをクライアントシステム部430に通知する。その後、ステップS 1316へ進む。「サイズ要求（s）」でない場合には、ステップS 1314へ進む。

【0102】ステップS 1314では、要求されるデータの要求種類が「データ要求（r）」であるか否かをチェックする。「データ要求（r）」である場合には、ステップS 1315へ進み、データ管理モジュール412に依頼して、該当データファイルを取得する。その後、ステップS 1316へ進む。

【0103】ステップS 1316では、取得したデータファイルの処理（加工）を通信データ処理モジュール422に依頼する。この時、送受信データテーブル1100とセキュリティ管理テーブル1200と通信データ群1000との3つの情報に含まれるセキュリティの強さを参照して、もっとも強い値を指定する。3つの情報すべてにセキュリティの強さに関する情報が存在しなければ、もっとも弱い値が指定されたとみなす。またこの時、送受信データテーブル1100のファイル形式やファイルサイズの情報があれば、これも指定する。また、暗号化処理などを行う際の暗号鍵や透かしデータなど必要に応じて指定する。通信データ処理モジュール422は、これら与えられたセキュリティの強さなどの情報を基にしてファイルの加工（処理）を行う。ここでファイルの加工とは、ファイルの圧縮、暗号化、画像データに対する透かしデータの付加、又はこれらの組み合わせからなる。この部分の処理の詳細については後述する。

【0104】次に、ステップS 1317では、データ通信モジュール424に対し、このファイルを公開ディレクトリ425に公開するよう依頼する。この処理を持ってデータの公開が完了し、クライアントシステム部430からのデータの取得が行えるようになる。

【0105】次に、ステップS 1318では、クライアントシステム部430に対して、データの準備が完了したことを、アクセストークンシード、保管した公開ディレクトリ425の場所、通信データサイズ、通信データ情報、セキュリティ情報などとともに通知し、通知内容に従って通信管理記憶装置423の送受信データテーブル1100を更新する。また、送受信データテーブル1100の送受信ステータス1102は、送受信中に設定される。その後、処理を終了する。

【0106】クライアントシステム部430は、アクセストークンシード等と共に準備が完了したことを受信し、そのアクセストークンシードを基に所定の演算を行ってアクセストークンを生成する。そして、クライアントシステム部430は、次回からはそのアクセストークンと共に通信を行うことができる。その際、図13では、アクセストークンが適切であるとしてステップS 1

301、S 1303、S 1304を通過し、所定の要求処理が実行される。

【0107】クライアントシステム部430が公開ディレクトリ425のデータを取得した後に、サーバシステム部400に取得が完了したことを通知した場合にもステップS 1301から1307までと同様のセキュリティ処理を行う。但し、この場合にはステップS 1307で要求されるデータの種類についての判断をする代わりに、通信データ群1000の要求内容がデータ取得の完了通知であるか否かを判断する。この処理は、ステップS 1307で通信データ群1000の要求内容を判断することにより、同一の処理ステップで処理できるが、本実施例では説明を簡略化するため、図13で示すフローチャートにはこれを含めていない。

【0108】通信データ群1000の要求内容がデータ取得完了通知である場合、通信管理モジュール421は最初に送受信データテーブル1100の送受信ステータス1102を送受信完了に更新する。次に、送受信データテーブル1100のセキュリティの強さが特定の値であった場合に、直ちに公開ディレクトリ425上の公開ファイルを削除する。特定の値とは、あらかじめ設定された範囲のセキュリティの強さに該当する場合、もしくは、プログラムの規定値を意味する。これに該当しない場合は、直ちに削除されずに、公開ディレクトリ425上に残される。

【0109】公開ディレクトリ425上にデータが残されている場合、ステップS 1315で該当するデータファイルを取得する処理と、ステップS 1316でデータファイルの処理（加工）を通信データ処理モジュール422に依頼する処理と、ステップS 1317でファイルを公開ディレクトリ425に公開するよう依頼する処理を省略することが出来る。データファイルが同じであり、かつセキュリティの強さなどの通信データ処理モジュール422に指定する情報が等しい場合にはこれらのステップを省略し、直ちにステップS 1318のクライアントシステム部430への通知処理を行う。

【0110】＜公開ディレクトリの監視処理＞公開ディレクトリ425に公開され、クライアントシステム部430がデータを取得した後も削除されずに残された公開ファイルは、前述したように再利用される場合がある。この再利用可能なファイルは、通信管理モジュール421の監視処理によって一定の条件によって削除される。なお、この監視処理はあらかじめ設定された時間間隔で、定期的に行われるが、任意に行っても良い。

【0111】監視処理は、実行されると、最初に通信管理記憶装置423の送受信データテーブル1100に記録されたセキュリティの強さを参照し、そのセキュリティの強さに対してあらかじめ設定されている期間以上に公開されているファイルを削除する。この処理によつて、クライアントシステム部430は、公開ディレクト

リ425のデータを取得した後も引き続き残されている公開ファイルであって一定期間以上利用されていないファイルを削除するだけでなく、セキュリティの強さが、特定の公開ファイルで、クライアントシステム部430が取得を完了したことを通知しないために、一定期間以上公開されることが望ましくないと設定されているファイルが残されていた場合にも削除することができる。

【0112】次に、あらかじめ設定された公開ディレクトリ425の最大記憶容量と公開ディレクトリ425の実際に使用されている記憶容量を比較する。もし、実際に使用されている記憶容量が最大記憶容量を越えていた場合には、すでにクライアントシステム部430から取得完了済みで、かつ、最も長い時間再利用されていない公開ファイルを、通信記憶管理装置423の送受信データテーブル1100上に記憶された公開ファイル425の情報（通信データ構成情報1106）と比較し、比較結果に応じて削除する。

【0113】以上の処理によって、利用者を特定するIDや要求されるセキュリティの強さ、公開されるデータの特性（ファイル形式やファイルの大きさなど）、公開されている時間、通信の状態などに従って、クライアントシステム部430から要求されるデータは管理される。一方、圧縮、暗号化、画像データに対する透かしデータの付加、およびこれらの組み合わせからなる加工が施されたファイルを公開ディレクトリ425から取得したクライアントシステム部430は、取得したファイルが必要に応じて再加工することができる。

【0114】すなわち、クライアントシステム部430の通信データ処理モジュール434は、データ通信モジュール424によって取得された通信データ群1000に含まれるセキュリティ情報などに従って、透かしデータの除去、復号化、圧縮データの伸張などを、必要に応じて処理することができる。

【0115】＜データファイルの加工処理＞先にも述べたように、通信管理モジュール421は、データファイルの加工を通信データ処理モジュール422に依頼する。この時、通信管理モジュール421は、セキュリティの強さ、ファイル形式、ファイルサイズの情報があればこれらも指定する。また暗号化処理などを行う際の暗号鍵や透かしデータなどを必要に応じて指定する。

【0116】通信データ処理モジュール422は、これらの与えられた情報を基にファイルの加工を行う。ここで、ファイルの加工とは、ファイルの圧縮、暗号化、画像データに対する透かしデータの付加、又はこれらの組み合わせからなる。図15は、クライアントシステム部430からデータ要求を受けて、サーバシステム部400の通信データ処理モジュール422が行うファイルの加工の処理を示すフローチャートである。

【0117】ステップS1501では、通信データ処理モジュール422が、データファイル、セキュリティの

強さ、ファイル形式、ファイルサイズ、暗号鍵、透かしデータまたはこれらの一部を取得する。これらは、通信管理モジュール421から与えられるが、必ずしもすべての項目が必須ではない。特に、暗号鍵や透かしデータなどは、セキュリティの強さやファイル形式に応じて使用されないことがあるため不要となる場合がある。

【0118】次に、ステップS1502では、ファイル形式が与えられているか否かを判断する。与えられている場合には、ステップS1504へ進む。与えられていなければ、ステップS1503へ進む。ステップS1503では、データファイルを読んで、データ形式を取得し、ステップS1504へ進む。データ形式が与えられていなければ、このステップS1503はなくても良い。データ形式は、実際にファイルを読み込んで、特定のファイル形式に固有な情報が含まれているか否かで判断し、あらかじめ決められた既知の形式であればこれを記憶する。たとえば、JIFやTIFFといった画像形式やZIPといった圧縮形式のファイル形式については、よく知られたアルゴリズムでこのファイル形式を判断することができる。

【0119】ステップS1504では、ファイルサイズが与えられているか否かをチェックする。ファイルサイズが与えられていれば、ステップS1506へ進む。ファイルサイズが与えられていなければ、ステップS1505でデータファイルからファイルサイズを取得し、ステップS1506へ進む。

【0120】ステップS1506では、透かしデータを付与することができるか否かを判断する。これは画像形式が透かしデータを付与することが可能な形式で、かつファイルサイズが透かしデータ付与可能なサイズより大きく、かつセキュリティの強さが透かしデータ付与が必要であるとして設定された値の範囲であり、かつ透かしデータが与えられているか否かで判断される。但し、透かしデータが与えられていない場合でもあらかじめ設定された透かし情報があれば透かしデータが与えられたものとみなす。また、透かしデータ付与について必要なセキュリティの強さがまったく設定されていない場合には、この判断結果は否となり、判断そのものが必須ではなくなる。

【0121】透かしデータを付与することができない場合には、ステップS1508へ進む。透かしデータを付与することができる場合には、ステップS1507へ進む。ステップS1507では、与えられた透かしデータを使用して、データファイルに透かしデータを付与する。ここで、セキュリティの強さによって、可視透かしデータ、不可視透かしデータ、またはその両方を付与する。その後、ステップS1508へ進む。

【0122】ステップS1508では、圧縮すべきか否かを判断する。これは、ファイルサイズがあらかじめ設定された値より大きく、かつファイル形式があらかじめ

設定された圧縮不要なファイル形式でないか否かで判断する。このとき、あらかじめ設定されたファイルサイズの値が0であっても良い。また、圧縮不要なファイル形式がまったく設定されていなくても良い。たとえば、あらかじめ設定されたファイルサイズが100バイトであり、実際のファイルサイズが16バイトであれば、判断結果は否となる。また、よく知られているように特定の画像形式は、一般的に知られた圧縮アルゴリズムでは圧縮効果を期待できないため、この画像形式をあらかじめ圧縮不要なファイル形式として設定していた場合には、この判断結果は否となる。

【0123】圧縮すべきでないと判断された場合には、ステップS1510へ進む。圧縮すべきであると判断された場合には、ステップS1509へ進む。ステップS1509では、図14に示す圧縮アルゴリズムテーブル1400を用いる。圧縮アルゴリズムテーブル1400は、ファイル形式1401と圧縮モジュール1402を対応付けて記憶する。ステップS1509では、図14に示す圧縮アルゴリズムテーブル1400を参照し、ファイル形式1401に応じた圧縮モジュール1402で

ファイルを一時記憶領域上で圧縮処理し、ステップS1510へ進む。

【0124】このとき、一時記憶領域上で圧縮された結果として、圧縮効果が見られなかった場合には、圧縮処理を中止し、入力ファイルを結果として使用し、一時記憶領域に非圧縮フラグ(n)を記憶する。圧縮効果があった場合には、圧縮フラグ(y)を記憶する。なお、圧縮アルゴリズムテーブル1400の参照は、本実施例では必須ではない。圧縮アルゴリズムテーブル1400を参照する代わりに、決められた特定の圧縮モジュール

を使用しても良い。この場合には、ファイル形式によって圧縮アルゴリズムは変わらず、常に同じ圧縮モジュールが使用される。

【0125】あらかじめ圧縮すべきかどうかを判断すること、及び圧縮効果がなかった場合に圧縮処理を中止することにより、圧縮処理に関わる処理負荷を軽減するだけでなく、クライアントシステム部430で取得した圧縮ファイルを伸張する処理負荷をも軽減することができる。

【0126】また、圧縮対象となるファイルは、論理的なファイルであっても、物理的なファイルであっても一時記憶領域上に記憶されたファイルであっても良い。たとえば、透かしデータを付与した結果を一時記憶領域上に論理ファイルとして記憶していた場合には、これを使用しても良い。

【0127】ステップS1508で圧縮すべきでないと判断された場合には、一時記憶領域に非圧縮フラグ

(n)を記憶する。この時、圧縮処理は行われず。ステップS1510では、暗号化処理を行うか否かを判断する。これは、セキュリティの強さにより決定する。ま

た、ここで暗号化するレベルの判断も行い、そのレベルを一時記憶領域に記憶する。

【0128】暗号化処理を行わないと判断された場合には、処理を終了する。暗号化処理を行うと判断された場合には、ステップS1511へ進む。ステップS1511では、図16に示す暗号化モジュールテーブル1600を用いる。暗号化モジュールテーブル1600は、暗号化レベル1601と暗号化モジュール1602を対応付けて記憶する。ステップS1511では、暗号化モジュールテーブル1600を参照して、先に一時記憶領域に記憶したレベルを基に、暗号化レベル1601に応じた暗号化モジュール1602で暗号化を行う。セキュリティの強さにより暗号化モジュール1602を使い分け

ることにより処理負荷を軽減することができ、さらにクライアントシステム部430において復号化処理を行う際にも負荷を軽減することができる。たとえば、セキュリティの強さが低いデータファイルに対しては、簡易な暗号化をすることにより処理負荷を軽減できる。なお、暗号化モジュールテーブル1600の参照は、本実施例では必須ではない。暗号化モジュールテーブル1600を参照する代わりに、決められた特定の暗号化モジュールを使用しても良い。この場合には、レベルによって暗号化モジュールは変わらず、常に特定の暗号化モジュールが使用される。また、圧縮対象となるファイルは、圧縮処理と同様に、論理的なファイルであっても、物理的なファイルであっても一時記憶領域上に記憶されたファイルであっても良い。

【0129】＜印刷システム処理＞クライアントシステム部430がサーバシステム部400から取得したデータが画像データであった場合に、クライアントシステム部430の通信管理モジュール433がデータ通信モジュール431を介して印刷システム部440へ印刷依頼する際の処理の詳細について説明する。

【0130】図17は、印刷システム部440がデータを受け取る際の処理の流れを説明するフローチャートである。処理の説明を以下に図17を用いて説明する。まず、ステップS1701では、データ通信モジュール441が暗号化された情報を受信する。通信管理モジュール442は、その受信した暗号化情報を通信データ処理モジュール443に復号化させ、その復号化された情報を格納するようにデータ管理モジュール444に依頼する。この依頼により、通信データ処理モジュール443は暗号化情報の復号化を行い、データ管理モジュール444は復号化された情報をデータ記憶装置445に記録する。

【0131】次に、ステップS1702では、通信管理モジュール442が、データ記憶装置445内のデータを取り出し、格納する。この場合、取り出したデータが画像データの場合には画像データの種類によって、画像データ内に透かしデータが含まれている場合がある。通

信データ処理モジュール443が通信管理モジュール442に格納された情報を解釈した後に、データ管理モジュール444がデータ記憶装置445に追加するレコードを作成する。

【0132】次に、ステップS1703では、通信データ処理モジュール443が図21で後述するオーダ情報に含まれる画像データの実体を特定する処理を行う。その後、関連する画像データを多重化する。この多重化の処理は、印刷時の印刷用ファイルと印刷プレビュー用ファイルという2つの用途として使用するための処理も可能である。

【0133】次に、ステップS1704では、多重化された元の画像ファイルに透かしデータが含まれていれば、通信データ処理モジュール443がその透かしデータを画像ファイルから外す（削除する）。

【0134】次に、ステップS1705では、クライアントシステム部430のデータ管理モジュール435が、印刷システム部440のデータ通信モジュール441に全てのファイル（図19の送受信情報1900）を送信する。印刷システム部440のデータ通信モジュール441は、その全ての画像ファイルを受信する。通信データ処理モジュール443は、多重化されたファイルも含めて全ての画像ファイルに透かしデータが含まれているか否かを判断する。透かしデータが含まれていない場合にはステップS1706へ進み、透かしデータが含まれている場合にはステップS1708へ進む。

【0135】ステップS1706では、通信データ処理モジュール443が、透かしデータが含まれていないファイルに対して、印刷に必要な画像処理を施し、ステップS1707へ進む。

【0136】ステップS1707では、通信データ処理モジュール443が上記の画像処理結果のファイルに対して暗号化する。この暗号化処理によって印刷直前まで画像ファイルは保護される。その後、ステップS1709へ進む。

【0137】ステップS1708では、通信データ処理モジュール443が、透かしデータが含まれているファイルに対しても同様の画像処理を行い、ステップS1709へ進む。

【0138】このようにして、ステップS1706において透かしデータが含まれていないファイルは画像処理され、ステップS1707ではそのファイルが暗号化され、印刷用ファイルが作成される。また、ステップS1708では透かしデータが含まれている印刷プレビュー用ファイルが作成される。

【0139】次に、ステップS1709では、ここまでのステップの処理でエラーが発生したか否かを判断する。エラーが発生した場合には、ステップS1710へ進む。エラーが発生していない場合には、ステップS1711へ進む。

【0140】ステップS1710では、画像処理中の障害により一時ファイルではない正しい拡張子の画像ファイルが残されることを防ぐために、処理中に作成された中間ファイルをすべて削除し、ステップS1702へ戻って未解決のデータに対して処理を再開する。

【0141】ステップS1711では、印刷システム部440の通信管理モジュール442が、以上の画像処理がなされた結果ファイル群を格納するようにデータ管理モジュール444に依頼する。データ管理モジュール444は、そのファイル群をデータ記憶装置445に図20で後述する画像実体情報（図20の画像テーブル）として格納する。

【0142】次に、ステップS1712では、以上の処理完了の状態をクライアントシステム部430に送信する。クライアントシステム部430は、その処理完了の状態をデータ記憶装置436に格納する。以上で、処理が終了する。

【0143】＜印刷処理＞図18は、印刷システム部440がデータ記憶装置445に格納されたファイルの印刷について行う処理を説明するためのフローチャートであり、オペレータの指示により行われる処理である。

【0144】ここでは、暗号化、透かしデータ等の処理をするための画像のデータ形式を例に述べているが、もちろん他の形式のデータにも当てはまるものである。まず、ステップ1801では、印刷システム部440の通信管理モジュール442がデータ管理モジュール444を介してデータ記憶装置445から印刷データを取り出す（読み出す）。この印刷データは、図17のステップS1706またはS1708で画像処理を施された印刷データである。

【0145】次に、ステップ1802では、通信管理モジュール442がデータ記憶装置445に格納されたファイルの実体の場所が特定（解決）されているか否かを判断する。特定されていなければステップ1803へ進み、特定されていればステップ1804へ進む。

【0146】ステップ1803では、図17のステップS1702の処理と同様な処理によりファイルの実体の場所を特定し、印刷に使用するデータの解決を図る。その後、ステップ1804へ進む。

【0147】ステップ1804では、ファイルが暗号化されているか否かを判断する。暗号化されていればステップ1805へ進み、暗号化されていなければステップ1806へ進む。

【0148】ステップ1805では、通信データ処理モジュール443がファイルをコピーして復号化する。この場合、暗号化をするか否かの判断はもちろん、どの暗号レベルを使用するかを判断する情報を画像そのものに持たせることも、別のファイルに保持させることも可能である。その後、ステップ1806へ進む。

【0149】ステップ1806では、ファイルに透かし

しデータが含まれているか否かを判断する。透かしデータが含まれている場合にはステップ1807へ進み、透かしデータが含まれていない場合にはステップ1808へ進む。

【0150】ステップ1807では、通信データ処理モジュール443がファイルから透かしデータを外す（削除する）。この場合、透かしデータが含まれているか否かの判断はもちろん、不可視透かしデータ、可視透かしデータを付与するか否かの情報を画像そのものに持たせることも、別のファイルに保持することも可能である。その後、ステップ1808へ進む。

【0151】ステップ1808では、全ファイルの画像処理が必要か否かを判断する。必要であればステップ1809へ進み、必要でなければステップ1810へ進む。ステップ1809では、通信データ処理モジュール443が、全ファイルについて画像処理を行う。その後、ステップ1810へ進む。

【0152】ステップ1810では、データ管理モジュール444がデータ記憶装置445にデータを格納し、通信管理モジュール442が印刷依頼処理をする。例として、印刷システム部440の画像処理モジュール446にデータの格納を依頼する通知をし、ユーザインタフェース装置（表示装置）447に取得データを表示するという動作を行わせることができる。あるいは、画像処理モジュール446がユーザインタフェース装置447からデータを取得し、印刷装置448に出力を行ったり、ユーザインタフェース装置447に表示せず、直接印刷装置448から出力することも可能である。

【0153】次に、ステップ1811では、データ管理モジュール444が、ステップ1805でコピーしたファイルを削除する。次に、ステップ1812では、印刷システム部440のデータ通信モジュール441が、印刷を完了した旨の通知をクライアントシステム部430のデータ通信モジュール431へと通知（送信）する。以上で、処理が終了する。

【0154】＜送受信情報＞図19は、送受信情報の構成の一部を示す図である。送受信情報1900は、クライアントシステム部430から印刷システム部440に渡される印刷に必要な情報が記載されている情報であり、画像情報1901を含む。

【0155】画像情報1901には、様々な種類の画像が含まれる。ビットマップを始め、JPEG、TIF、ZIP等のどのフォーマットの画像データを用いても本実施例を適用できることはいふまでもない。

【0156】＜画像テーブルの構成＞図20は、画像テーブルの構成を示す図である。画像テーブル2000は、クライアントシステム部430のデータ記憶装置436ならびに印刷システム部440のデータ記憶装置445に保持される。画像テーブル2000は、画像ID、ファイル名称、ファイル実体パス、更新日付とい

た画像の実体情報を管理する為に必要な情報を保持する。

【0157】＜オーダ情報＞図21は、オーダ情報の構成の一部を示したものである。オーダ情報2105は、オーダID2101、オーダ状況2102、印刷ファイルID2103、及び印刷ファイルサイズ2104を有する。オーダID2101は、印刷注文を特定するIDと等価な情報である。オーダ状況2102は、おおまかに印刷待ち、印刷中、印刷完了などのステータスが設定される。印刷ファイルID2103は、印刷するファイルを特定するIDと等価な情報であり、複数の場合もある。印刷ファイルサイズ2104は、印刷ファイルID2103に対応するファイルのサイズに相当する。

【0158】本実施例によれば、クライアントシステム部430からサーバシステム部400にデータが要求された時点で、まずIDやパスワードやセキュリティの強さや要求内容といった情報を取得し、その情報に基づいて最適な画像データの加工処理を行って公開ディレクトリ425に公開する。クライアントシステム部430の受信時に復号化を自動的に行うことによって、ネットワーク上の画像データと公開ディレクトリ425上の画像データを同時に保護しながら、処理負荷を軽減することができる。

【0159】また、クライアントシステム部430からサーバシステム部400にデータを送信する際にも同様に、データの最適な加工処理を選択し、公開ディレクトリ425上に転送された画像データを自動的に復号化しながら安全なサーバシステム部400に移動させることにより、処理負荷を軽減することができる。

【0160】さらに、画像データのセキュリティの強さによって、暗号の復号化、透かしデータの除去などの処理を印刷直前にするか、または予めしておくかという判断ができる。これによって、画像データの安全性が保たれ、しかも印刷依頼から印刷処理までの負荷を軽減することができる。

【0161】なお、ネットワークは、インターネット（公開ネットワーク）が好ましく、通信プロトコルはファイル転送プロトコル（FTP）が好ましい。

【0162】上述した実施例による情報処理装置（印刷システム、サーバコンピュータ、クライアントコンピュータ）に対し、上記実施例の機能を実現するためのソフトウェアのプログラムコードを供給し、その情報処理装置（CPUあるいはMPU）に格納されたプログラムに従って動作させることによって実施することができる。

【0163】この場合、上記ソフトウェアのプログラムコード自体が上述した実施例の機能を実現することになり、そのプログラムコード自体、およびそのプログラムコードを情報処理装置に供給するための手段、例えばかかるプログラムコードを格納した記録媒体は本発明を構成する。かかるプログラムコードを記憶する記録媒体と

しては、例えばフロッピーディスク、ハードディスク、光ディスク、光磁気ディスク、CD-ROM、磁気テープ、不揮発性のメモ리카ード、ROM等を用いることができる。

【0164】また、情報処理装置が供給されたプログラムコードを実行することにより、上述の実施例の機能が実現されるだけでなく、そのプログラムコードが情報処理装置において稼働しているOS（オペレーティングシステム）あるいは他のアプリケーションソフト等と共同して上述の実施例の機能が実現される場合にもかかるプログラムコードは本発明の実施例に含まれることは言うまでもない。

【0165】さらに、供給されたプログラムコードが情報処理装置の機能拡張ボードや情報処理装置に接続された機能拡張ユニットに備わるメモリに格納された後、そのプログラムコードの指示に基づいてその機能拡張ボードや機能拡張ユニットに備わるCPU等が実際の処理の一部または全部を行い、その処理によって上述した実施例の機能が実現される場合にも本発明に含まれることは言うまでもない。

【0166】なお、上記実施例は、何れも本発明を実施するにあたっての具体化のほんの一例を示したものに過ぎず、これらによって本発明の技術的範囲が限定的に解釈されてはならないものである。すなわち、本発明はその精神、またはその主要な特徴から逸脱することなく、様々な形で実施することができる。

【0167】

【発明の効果】以上説明したように本発明によれば、印刷データを保護して記憶装置内に保管することにより、印刷データの安全性が保たれ、印刷依頼から印刷処理までの負荷を軽減することができる。

【図面の簡単な説明】

【図1】本実施例によるネットワークシステムの構成図である。

【図2】本実施例によるクライアントコンピュータ及びサーバコンピュータの構成図である。

【図3】本実施例による印刷システムの構成図である。

【図4】本実施例によるネットワークシステムのモジュール構成図である。

【図5】本実施例のクライアントシステム部とサーバシステム部間のデータ処理のフローチャートである。

【図6】本実施例の通知を受けたクライアントシステム部の処理のフローチャートである。

【図7】本実施例の通知を受けたサーバシステム部の処理のフローチャートである。

【図8】本実施例のサーバシステム部の公開ディレクトリ割り当て処理のフローチャートである。

【図9】本実施例の公開ディレクトリ割り当て準備が完了した通知を受けたクライアントシステム部の処理のフローチャートである。

【図10】本実施例の通信データ構成図である。

【図11】本実施例の送受信データテーブルの構成図である。

【図12】本実施例のセキュリティ管理テーブルの構成図である。

【図13】本実施例のセキュリティ処理のフローチャートである。

【図14】本実施例の圧縮アルゴリズムテーブルの構成図である。

10 【図15】本実施例のデータファイルの加工処理のフローチャートである。

【図16】本実施例の暗号化モジュールテーブルの構成図である。

【図17】本実施例の画像データ処理のフローチャートである。

【図18】本実施例の印刷処理のフローチャートである。

【図19】本実施例の送受信情報の構成図である。

【図20】本実施例の画像テーブルの構成図である。

20 【図21】本実施例のオーダ情報の構成図である。

【符号の説明】

100 サーバコンピュータ

110～11N クライアントコンピュータ

120～12N 印刷システム

200 入出力バス

201 CPU

202 RAM

203 ROM

204 ネットワークインターフェイス（NETIF）

30 205 ビデオRAM（VRAM）

206 CRT

207 キーボードコントローラ（KBC）

208 キーボード（KB）

209 ハードディスクドライブ（HDD）

210 リムーバブルディスクドライブ（FDD）

300 入出力バス

301 CPU

302 RAM

303 ROM

40 304 ネットワークインターフェイス（NETIF）

305 ビデオRAM

306 CRT

307 キーボードコントローラ（KBC）

308 キーボード（KB）

309 ハードディスクドライブ（HDD）

310 リムーバブルディスクドライブ（FDD）

311 プリンタ制御装置（PRTC）

312 プリンタ

313 拡張外部入出力装置制御装置（CTLR）

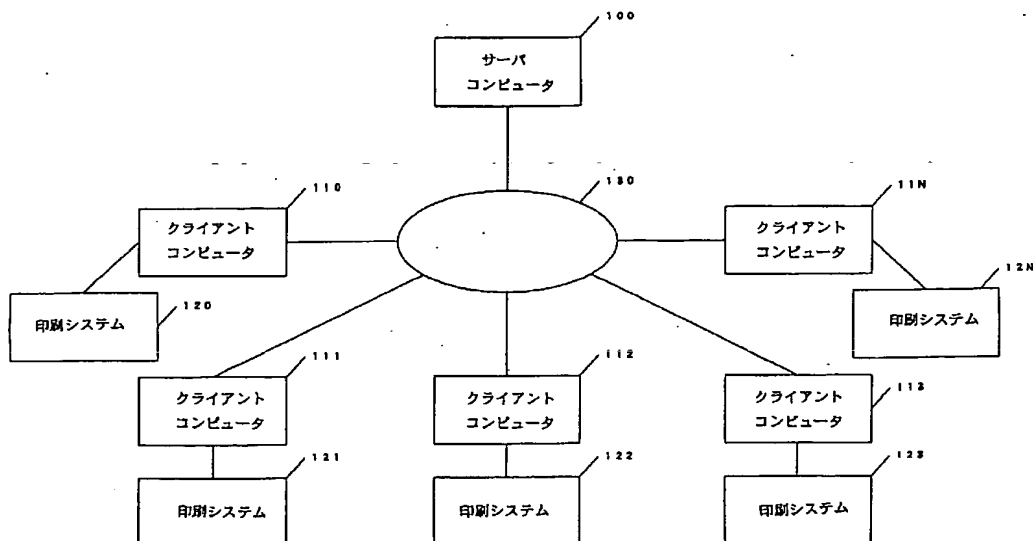
50 314 拡張外部入出力装置（スキャナ）



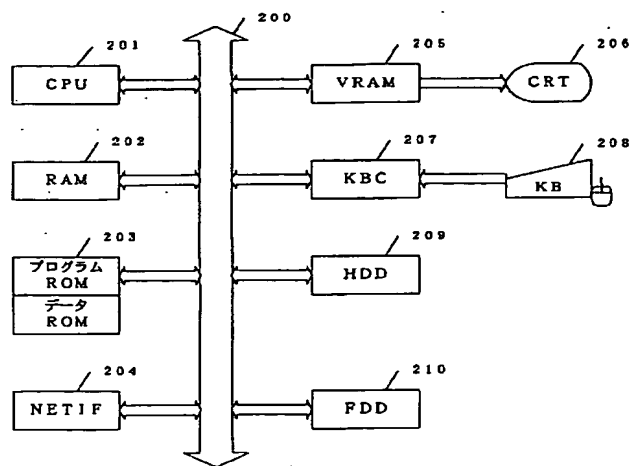
400 サーバシステム部  
 410 データ保管サーバシステム部  
 411 データ記憶装置  
 412 データ管理モジュール  
 420 データ公開・通信サーバシステム部  
 421 通信管理モジュール  
 422 通信データ処理モジュール  
 423 通信管理記憶装置  
 424 データ通信モジュール  
 425 公開ディレクトリ  
 430 クライアントシステム部  
 431 データ通信モジュール  
 432 通信管理記憶装置  
 433 通信管理モジュール  
 434 通信データ処理モジュール  
 435 データ管理モジュール  
 436 データ記憶装置  
 440 印刷システム部  
 441 データ通信モジュール  
 442 通信管理モジュール  
 443 通信データ処理モジュール  
 444 データ管理モジュール  
 445 データ記憶装置  
 446 画像処理モジュール  
 447 ユーザインターフェイス装置  
 448 印刷装置  
 1000 ID  
 1001 パスワード  
 1002 アクセストークン又はアクセストークンシー  
 ド

1003 要求内容  
 1004 セキュリティの強さ  
 1005 アプリケーションデータ  
 1100 送受信データテーブル  
 1101 ID  
 1102 送受信ステータス  
 1103 ファイル名特定情報  
 1104 セキュリティの強さ  
 1105 ファイル形式  
 10 1106 通信データ構成情報  
 1200 セキュリティ管理テーブル  
 1201 ID  
 1202 パスワード  
 1203 アクセストークン  
 1204 セキュリティの強さ  
 1205 要求日時  
 1400 圧縮アルゴリズムテーブル  
 1401 ファイル形式  
 1402 圧縮モジュール  
 20 1600 暗号化モジュールテーブル  
 1601 暗号化レベル  
 1602 暗号化モジュール  
 1900 送受信情報  
 1901 画像情報  
 2000 画像テーブル  
 2101 オーダID  
 2102 オーダ状況  
 2103 印刷ファイルID  
 2104 印刷ファイルサイズ  
 30 2105 オーダ情報

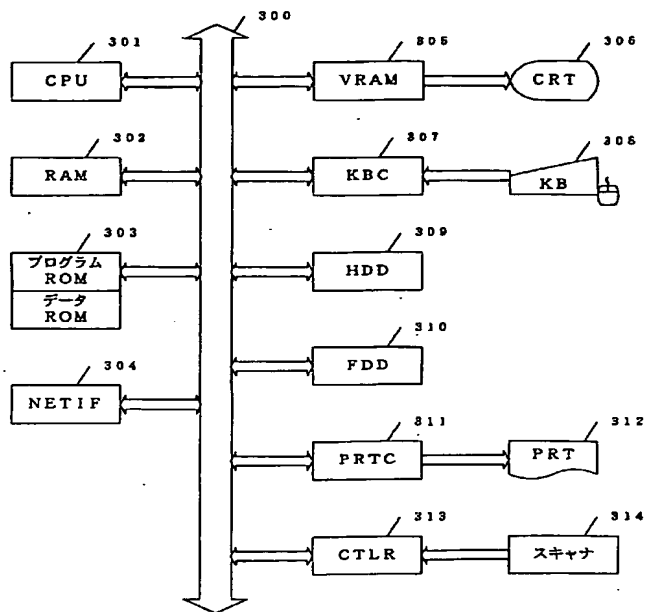
【図1】



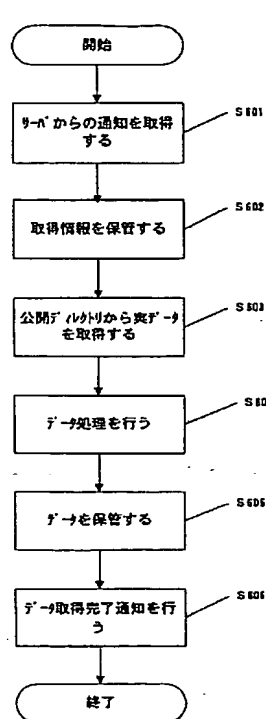
【図2】



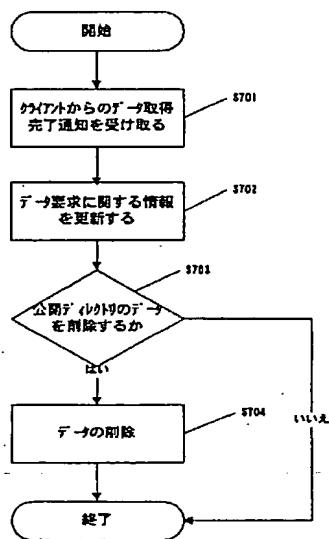
【図3】



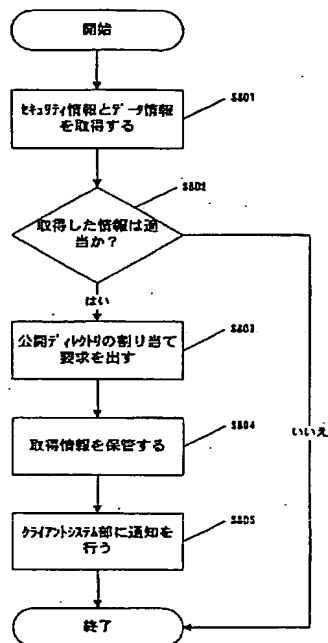
【図6】



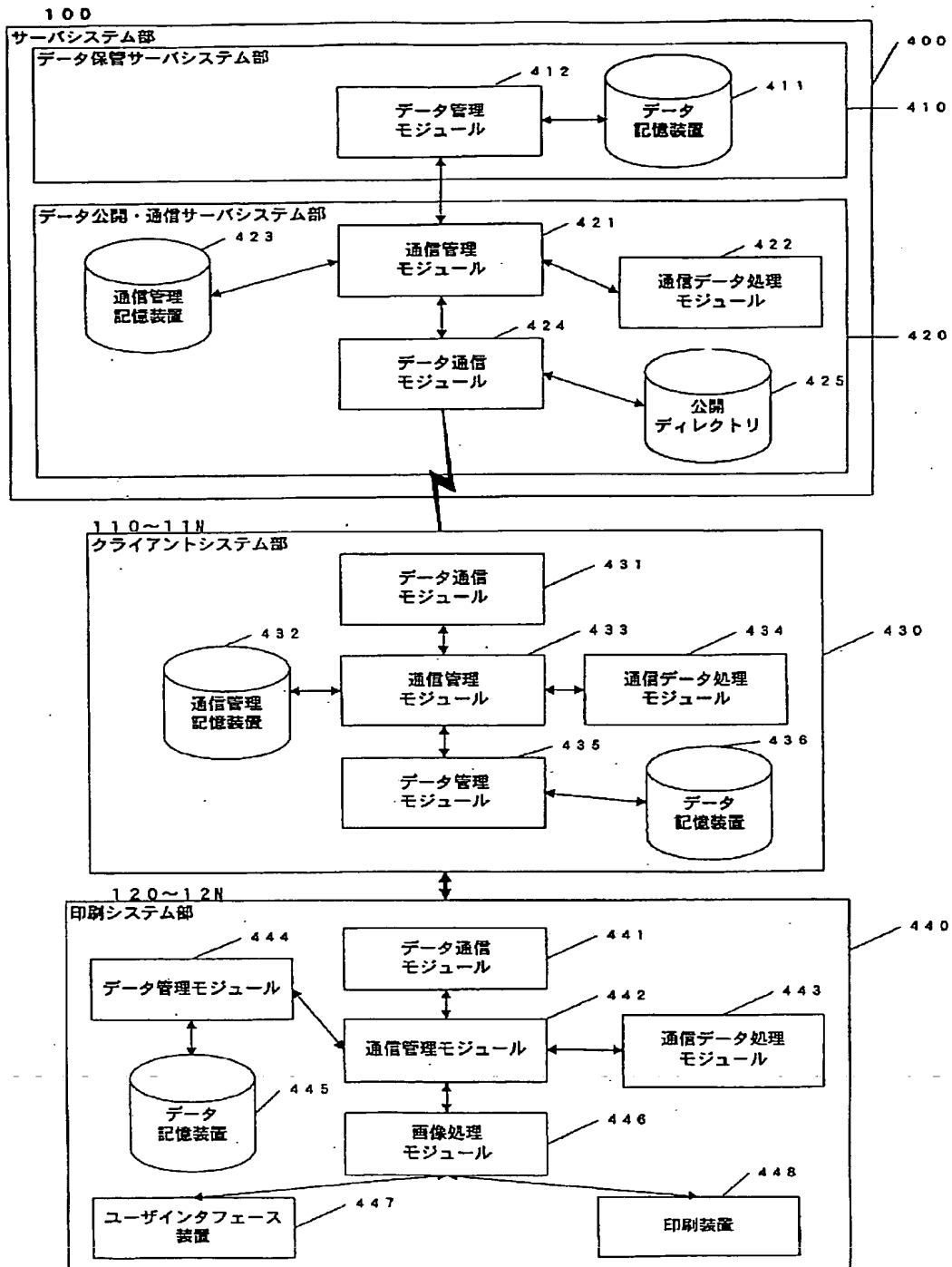
【図7】



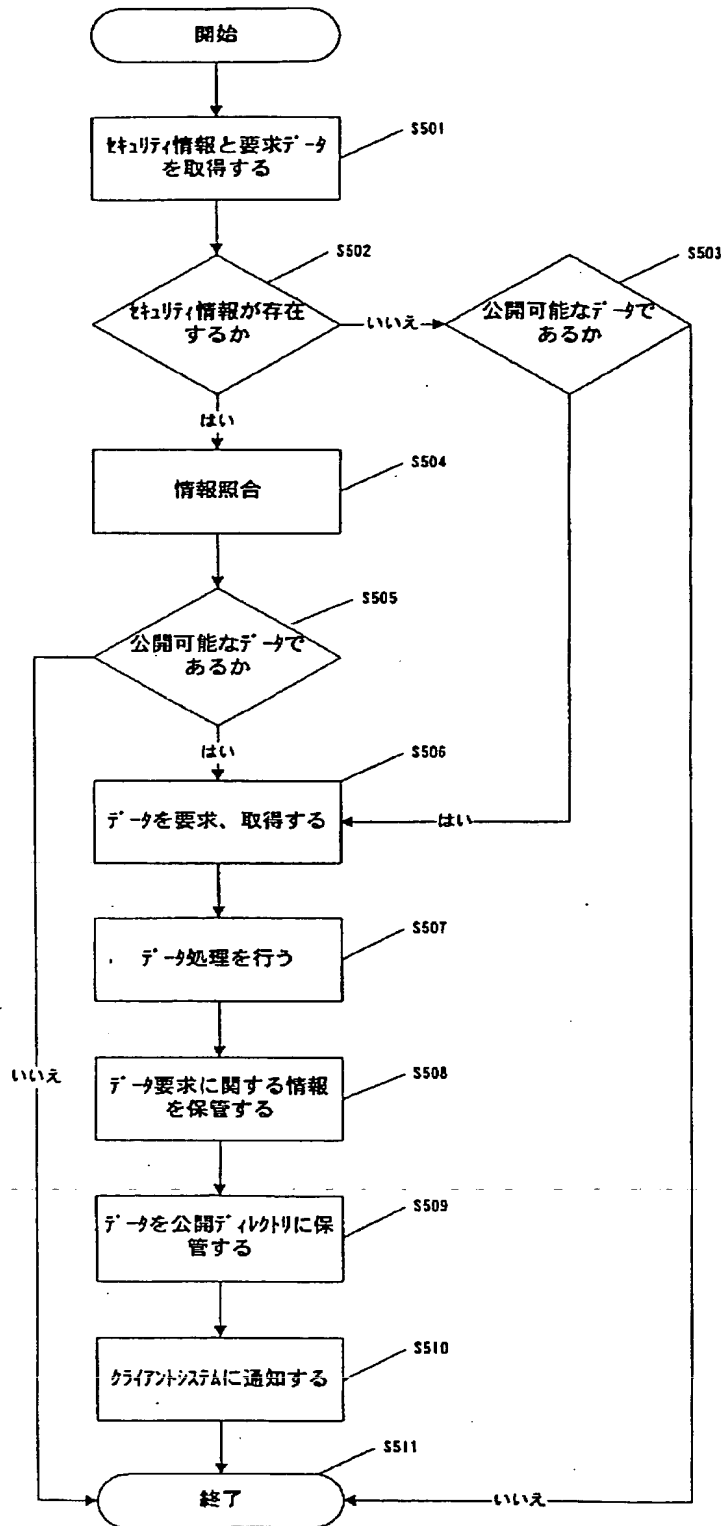
【図8】



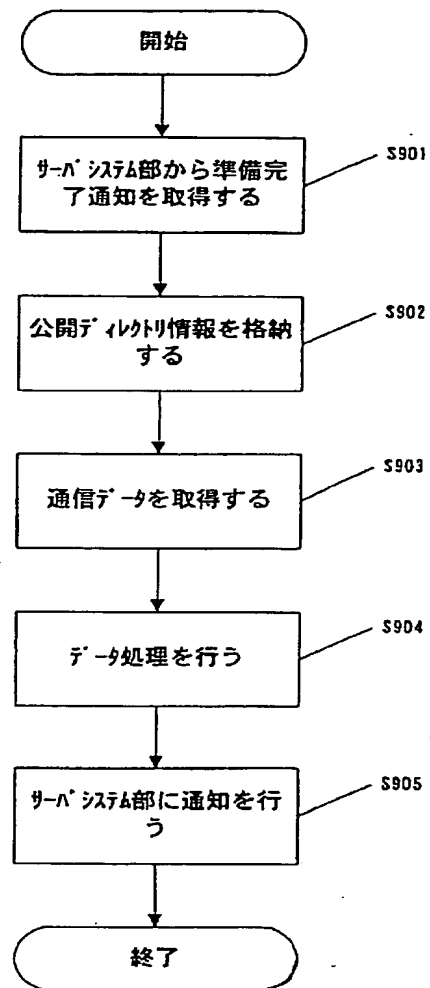
【図4】



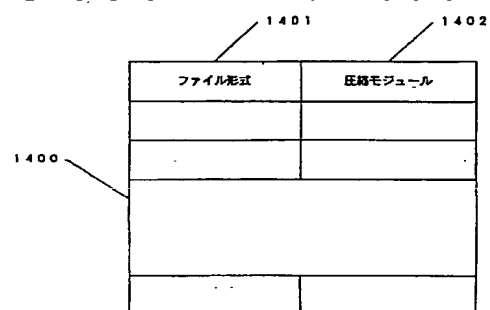
【図5】



【図9】



【図14】



【図10】

1000	1001	1002	1003	1004	1005
ID	アドレス	ファイル名 CB ファイルパス	要求内容	レスポンスの長さ	レスポンスデータ

【図11】

1100	1101	1102	1103	1104	1105	1106
ID	送信元アドレス	ファイル名特定情報	レスポンスの長さ	ファイル形式	送信データ復元情報	

【図20】

2000
画像テーブル
画像ID ファイル名称 ファイル実体パス 更新日付

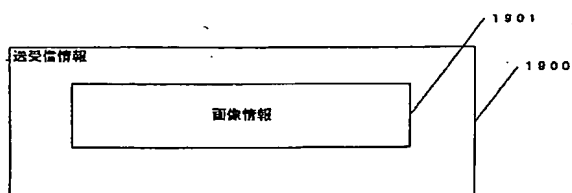
【図12】

1200	1201	1202	1203	1204	1205
ID	アドレス	ファイル名	レスポンスの長さ	要求日時	

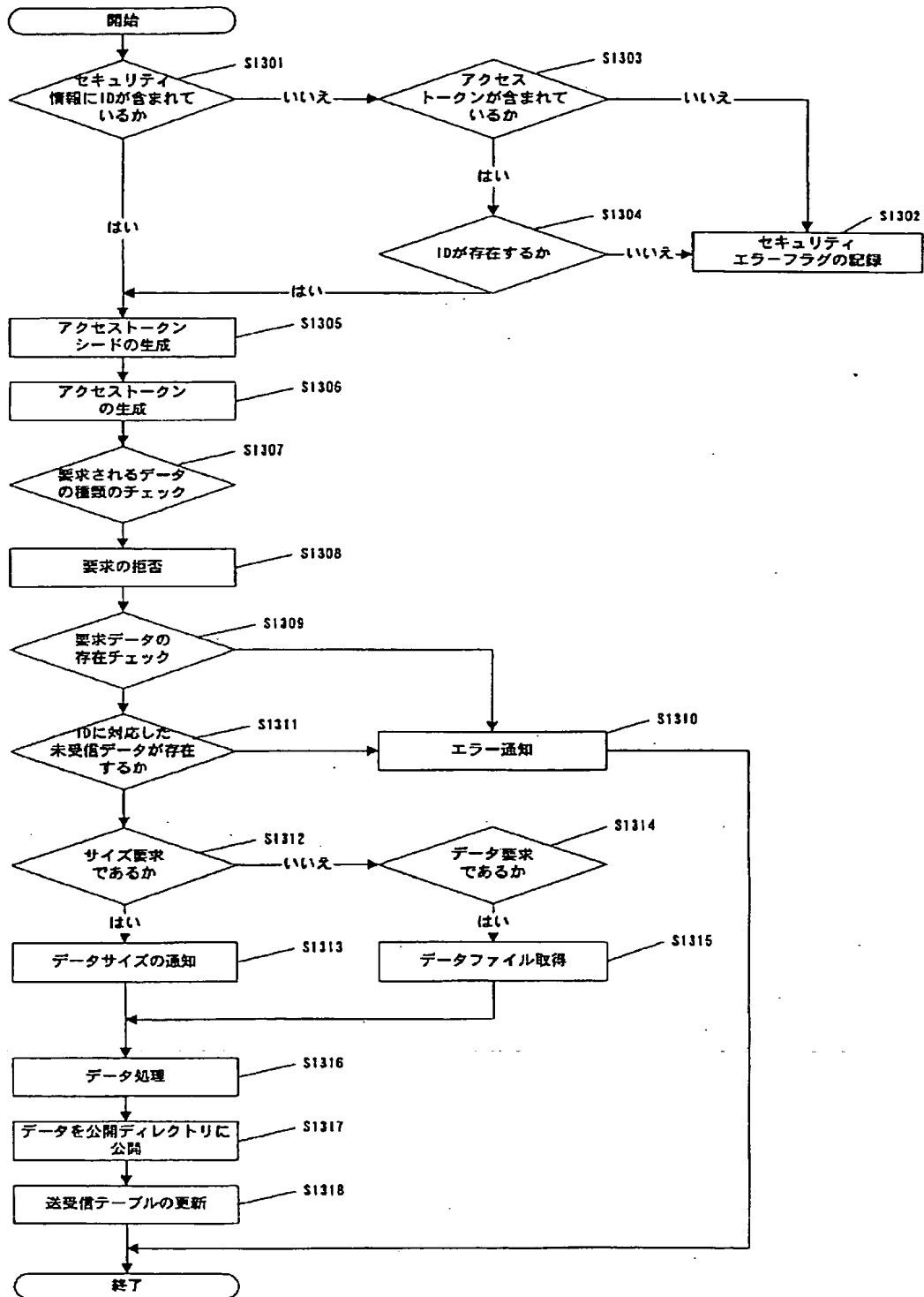
【図16】

1600	1601	1602
暗号化レベル	暗号化モジュール	

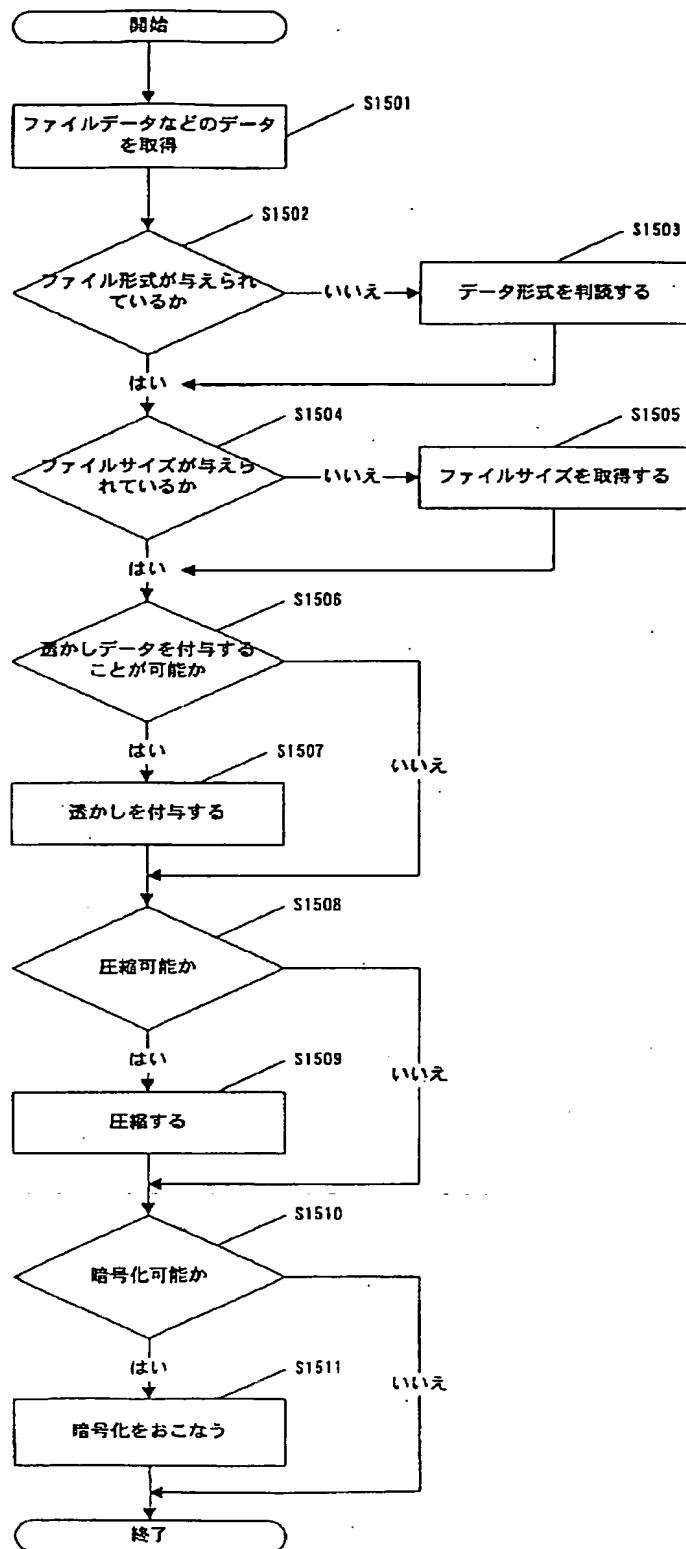
【図19】



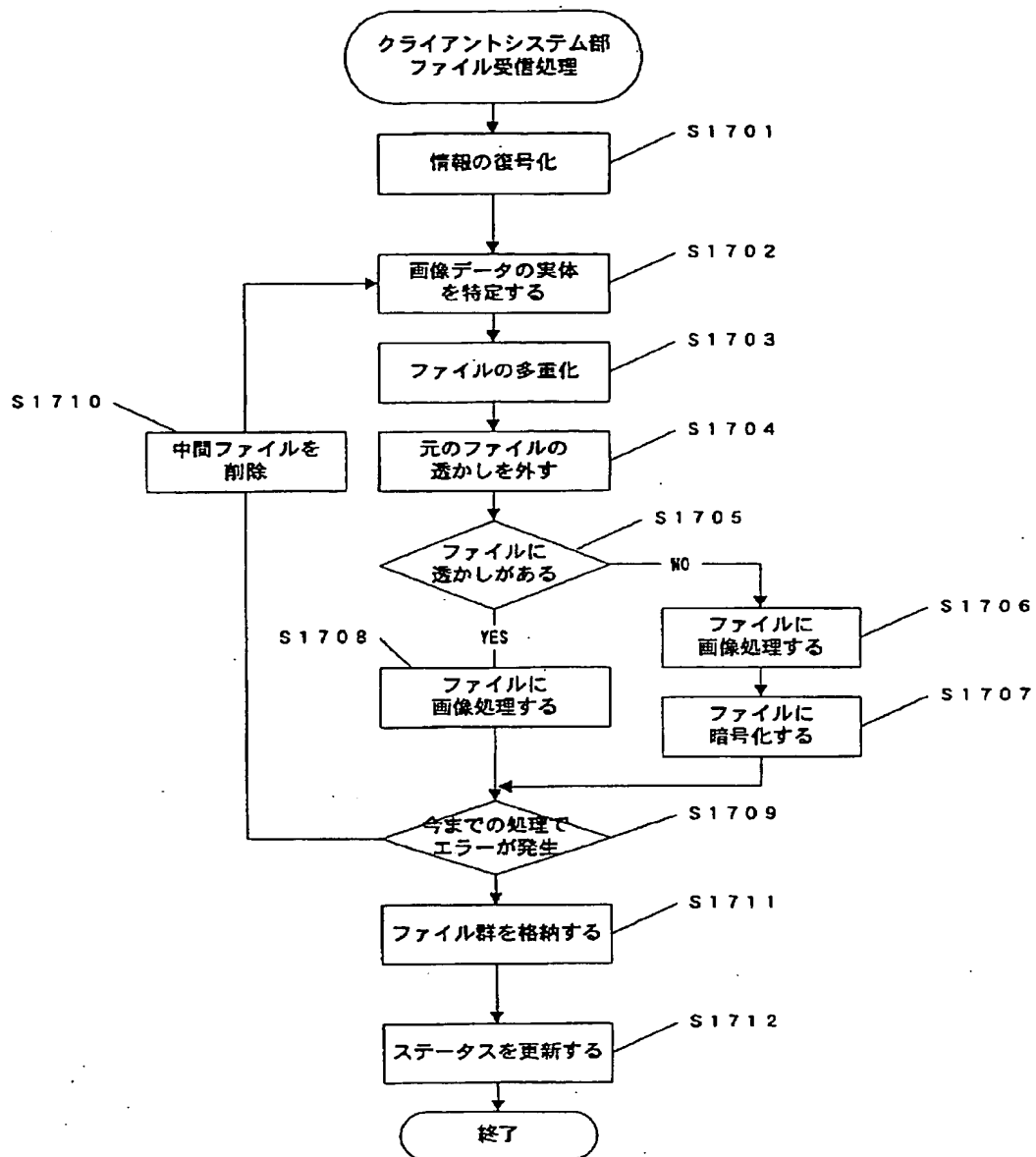
【図13】



【図15】

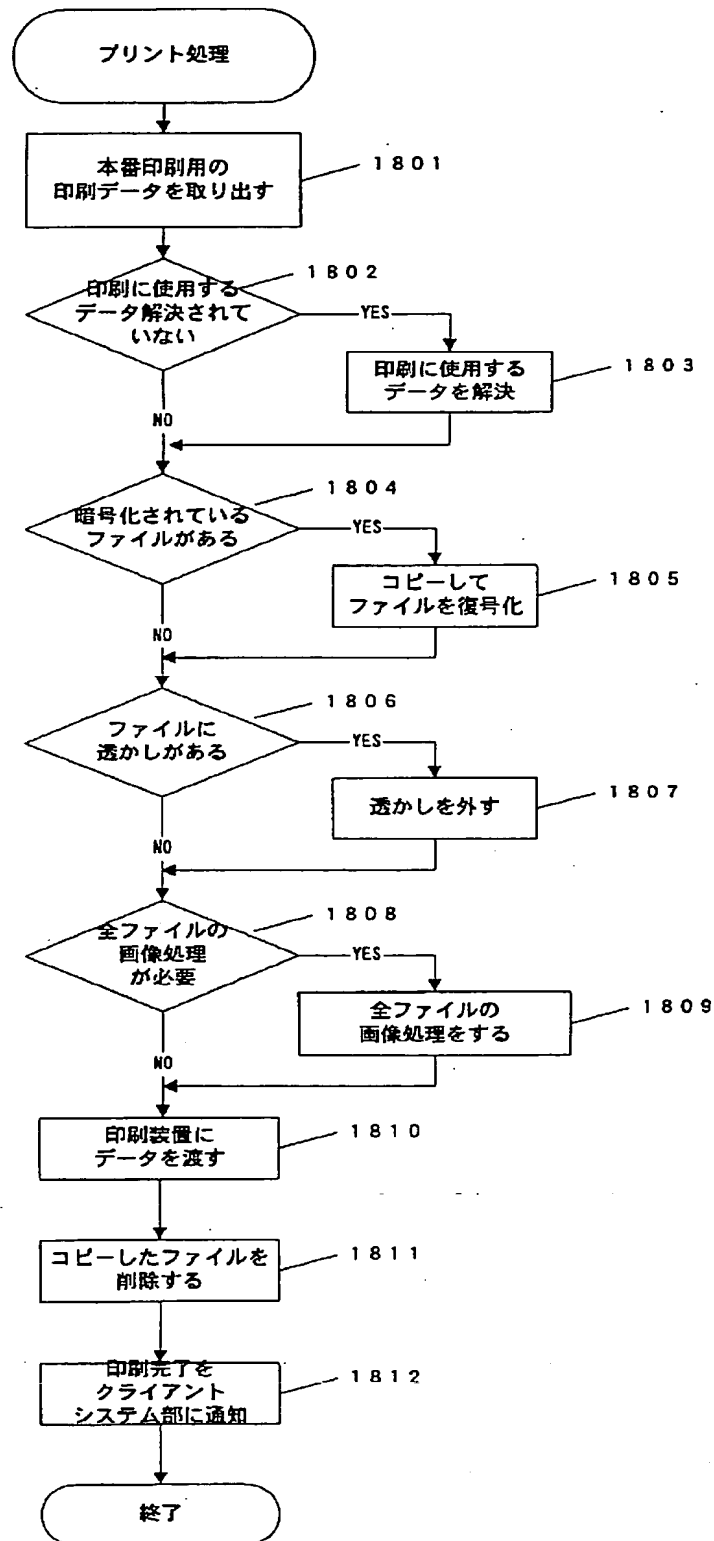


【図17】





【図18】



【図21】

	2101	2102	2103	2104
2105	オーダーID	オーダー状況	印刷ファイルID	印刷ファイルサイズ

---

フロントページの続き

(72)発明者 大嶋 肇  
 東京都大田区下丸子3丁目30番2号 キヤ  
 ノン株式会社内

(72)発明者 高久 雅彦  
 東京都大田区下丸子3丁目30番2号 キヤ  
 ノン株式会社内

Fターム(参考) 2C061 AQ06 AR01 HJ06 HQ12 HQ17  
 5B021 BB09 CC08 EE04 NN18  
 5B089 GA13 JA35 JB23 KA17 KB04  
 KC57 KH30 LB12